(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6198231号
(P6198231)

(45)発行日　平成29年9月20日(2017.9.20)　(24)登録日　平成29年9月1日(2017.9.1)

(51)Int.Cl.		F I		
H04L 9/10	(2006.01)	H04L	9/00	621A
G06F 21/31	(2013.01)	G06F	21/31	
G06F 21/62	(2013.01)	G06F	21/62	

請求項の数 8　(全 21 頁)

(21)出願番号	特願2014-556566 (P2014-556566)
(86)(22)出願日	平成25年1月28日 (2013.1.28)
(65)公表番号	特表2015-508257 (P2015-508257A)
(43)公表日	平成27年3月16日 (2015.3.16)
(86)国際出願番号	PCT/US2013/023353
(87)国際公開番号	WO2013/119401
(87)国際公開日	平成25年8月15日 (2013.8.15)
審査請求日	平成28年1月5日 (2016.1.5)
(31)優先権主張番号	13/370,232
(32)優先日	平成24年2月9日 (2012.2.9)
(33)優先権主張国	米国(US)

前置審査

(73)特許権者　314015767
マイクロソフト　テクノロジー　ライセンシング，エルエルシー
アメリカ合衆国　ワシントン州　９８０５２　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介

最終頁に続く

(54)【発明の名称】デバイスデータのためのセキュリティポリシー

(57)【特許請求の範囲】

【請求項１】

安全性に関連したタスクを管理及び／又は実行するセキュリティモジュール及びリカバリーモジュールを備えるデバイスの作動方法であって、

前記セキュリティモジュールによって、当該デバイスについてのセキュリティポリシーの違反を検出するステップと、

前記セキュリティモジュールによって、前記検出に応答して、当該デバイスのセキュリティ鍵を、該セキュリティ鍵を中間のセキュリティ鍵により暗号化することによって閉鎖するステップと、

前記リカバリーモジュールによって、前記閉鎖に応答して、ユーザが前記中間のセキュリティ鍵の場所を指定することを可能にするようにグラフィカルユーザインターフェースを当該デバイスに表示させるステップと、

前記リカバリーモジュールによって、前記中間のセキュリティ鍵が位置する保護された場所を特定する前記グラフィカルユーザインターフェースへのユーザ入力を受け取るステップと、

前記リカバリーモジュールによって、前記保護された場所から前記中間のセキュリティ鍵を取り出し、該取り出された中間のセキュリティ鍵が正しいかどうかを判定するステップと、

前記中間のセキュリティ鍵が正しい場合に、前記リカバリーモジュールによって、前記中間のセキュリティ鍵を用いて前記セキュリティ鍵を復号するステップと

を有し、
前記セキュリティポリシーは、当該デバイスについてのログオン失敗の閾回数を特定し、前記検出は、失敗した当該デバイスについてのログオンの回数が前記閾回数に達したと検出することを含み、失敗した当該デバイスについてのログオンの回数は、２又はそれ以上の異なるタイプの認証ファクタに基づく、方法。
【請求項２】
前記検出は、当該デバイスの信頼できるステータスが覆されたと検出することを含む、
請求項１に記載の方法。
【請求項３】
前記検出は、当該デバイスが遠隔のセキュリティサービスにチェックインできなかったと検出することを含む、
請求項１に記載の方法。
【請求項４】
前記検出は、当該デバイスの状態の変化を検出することを含み、該状態は、ハードウェア状態、ソフトウェア状態、又はネットワーク状態のうちの１つ以上を含む、
請求項１に記載の方法。
【請求項５】
安全性に関連したタスクを管理及び／又は実行するセキュリティモジュール及びリカバリーモジュールを備えるデバイスの作動方法であって、
当該デバイスが遠隔のセキュリティサービスにチェックインできなかったとのインジケーションを受け取ることに応答して、前記セキュリティモジュールによって、当該デバイスに属するセキュリティ鍵を閉鎖させるステップと、
前記セキュリティ鍵が閉鎖されるとのインジケーションに応答して、前記リカバリーモジュールによって、該閉鎖されたセキュリティ鍵を回復するためのリカバリー鍵を要求するリカバリープロシージャを起動するステップと、
前記リカバリーモジュールによって、正確なリカバリー鍵が前記リカバリープロシージャの部分として提供されるかどうかを判定するステップと、
前記正確なリカバリー鍵が提供される場合に、前記リカバリーモジュールによって、前記セキュリティ鍵が回復されることを可能にするステップと
を有する方法。
【請求項６】
前記セキュリティ鍵が閉鎖されるとの前記インジケーションは、当該デバイスについてのオペレーティングシステムデータが利用可能でないとのインジケーションを含む、
請求項５に記載の方法。
【請求項７】
前記セキュリティ鍵は、該セキュリティ鍵を暗号化することによって閉鎖され、前記正確なリカバリー鍵が提供される場合は、前記セキュリティ鍵は、中間のセキュリティ鍵を用いて当該デバイスのために復号される、
請求項５に記載の方法。
【請求項８】
前記遠隔のセキュリティサービスへの定期的なチェックインを試みるステップ
を更に有する請求項５に記載の方法。
【発明の詳細な説明】
【背景技術】
【０００１】
今日の個人は、様々なタスク、例えば、仕事に関連したタスク、個人的な活動、レクリエーション活動、等を行うために使用され得る多種多様のデバイスへのアクセスを有する。幾つかのデバイスは、仕事に関連した目的のような特定の目的に捧げられるが、多くのデバイスは、“混合用途”デバイスを考えられている。例えば、個人のスマートフォンは、個人的な電話呼び出しを行うこと、写真を撮ること、メッセージを送信すること、等の

ような個人的なタスクを行うために使用され得る。スマートフォンはまた、仕事に関連した電子メールを送受信すること、作業文書を読み編集すること、業務連絡を管理すること、等のような仕事に関連した活動のためにも使用されてよい。

【０００２】

そのような混合用途デバイスの１つの結果は、様々なタイプのデータが特定のデバイスに記憶され得ることである。例えば、仕事に関連した文書は、個人が文書を見るためにスマートフォンを使用することができるように、スマートフォンにおいて局所的に記憶され得る。デバイスにおいて局所的にデータを記憶することは、データへの使い勝手の良いアクセスを個人に提供することができるが、それはまた、考慮すべき安全上のリスクを提起することがある。例えば、デバイスに記憶されている極秘データは、潜在的に、そのデバイスの無許可の所持を得る個人に露わにされる可能性がある。

【発明の概要】

【発明が解決しようとする課題】

【０００３】

デバイスに記憶されているデータを保護するための幾つかの技術は、単にデータをデバイスから消去することによって、データへの試みられた無許可のアクセスのインジケーションに応答する。これは、無許可のアクセスからデータを保護するために特定の状況においては有効であり得るが、それはまた、重要なデータの喪失を生じさせ得る。例えば、子供がゲームで遊ぶために自身の親の電話へのアクセスを得ようと試みるシナリオを考える。電話に付随したセキュリティ機能、例えば、制限された再試行ロジック又はポリシー強制のための企業サーバは、この試みを、個人が極秘データへの無許可のアクセスを得ようとしているとして解釈することがある。これに応じて、セキュリティ機能は、電話にあるデータを消去させ得る。これは重要なデータの喪失を生じさせ得るのみならず、再構成プロセスがデバイスを機能状態へ戻すために実施され得る点で、考慮すべき不便さを与えうる。

【課題を解決するための手段】

【０００４】

この要約は、詳細な説明において以下で更に記載される簡略化された形において概念の選択を導入するよう設けられる。この要約は、請求される対象の重要な特徴又は必須の特徴を特定することを目的とせず、且つ、請求される対象の適用範囲を制限するために使用されることを目的としない。

【０００５】

デバイスデータのためのセキュリティポリシーを提供する技術が記載される。少なくとも幾つかの実施において、デバイスに関するデータは、暗号化された形で記憶される。デバイスの機能性（例えば、アプリケーション）によって利用されるために、暗号化されたデータは記憶装置から読み出され、復号化鍵を用いて復号され、その機能性へ提供される。暗号化されたデータが権限のないエンティティによって復号されることを防ぐよう、技術は、デバイスデータへの無許可のアクセスを得ようとする試みが検出される場合に、復号化鍵が閉鎖されることを可能にする。実施において、復号化鍵は、様々な方法において、例えば、復号化鍵を削除すること、暗号化鍵をメモリに上書きすること、暗号化鍵を暗号化すること、等によって、閉鎖され得る。

【０００６】

実施形態は、閉鎖された復号化鍵がリカバリーエクスペリエンスを介して回復されることを可能にする。例えば、リカバリーエクスペリエンスは、ユーザに高度な認証情報を要求する認証プロシージャを含むことができる。そのような高度な認証情報は、権限のあるユーザによって取り出され得る高エントロピーのリカバリーパスワードを含むことができる。ユーザが正確なリカバリーパスワードを提供する場合に、リカバリーエクスペリエンスは、閉鎖された復号化鍵を回復させる、例えば、脱閉鎖させる、ことができる。実施において、閉鎖された復号化鍵が回復された後、ユーザは、デバイスログインエクスペリエンスの部分のような、デバイスへの標準の認証情報を提供することができる。認証が成功

すると、回復された復号化鍵は、データがユーザ及び／又はデバイスの機能性によって“平文で（in the clear）”アクセスされ得るように、デバイスにおいてデータを復号するために使用され得る。

【０００７】

実施形態は、データに記憶されているデータを無許可のアクセスから保護するために使用され得るセキュリティポリシーを提供する。例えば、セキュリティポリシーは、特定の条件が存在する場合にデバイスのための復号化鍵が閉鎖されるべきであると特定することができる。そのような条件の例は、多数のデバイスログインの失敗、信頼できないデバイスにより暗号化されたデータにアクセスしようとする試み、復号化鍵及び／又は安全性に関連した信用証明物の明示的取り消し、特定の時点で“チェックイン”すべきデバイスの失敗、等に係ることができる。

【図面の簡単な説明】

【０００８】

詳細な説明は、添付の図を参照して記載される。図中、参照符号の最左の数字は、その参照符号が最初に現れる図を示す。異なる図における同じ参照符号は、類似する又は同じ項目を示す。

【０００９】

【図１】本願で論じられている技術を用いるよう動作可能な実施例における環境の説明である。

【００１０】

【図２】１又はそれ以上の実施形態に従う方法におけるステップを記載するフロー図である。

【００１１】

【図３】１又はそれ以上の実施形態に従う方法におけるステップを記載するフロー図である。

【００１２】

【図４】１又はそれ以上の実施形態に従う方法におけるステップを記載するフロー図である。

【００１３】

【図５】本願で記載される技術の実施形態を実施するよう構成される、図１を参照して記載される例となるシステム及びコンピュータデバイスを表す。

【発明を実施するための形態】

【００１４】

概要

デバイスデータのためのセキュリティポリシーを提供する技術が記載される。実施において、デバイスに関するデータは、暗号化された形で記憶される。デバイスの機能性（例えば、アプリケーション）によって利用されるために、暗号化されたデータは記憶装置から読み出され、復号化鍵を用いて復号され、その機能性へ提供される。暗号化されたデータが権限のないエンティティによって復号されることを防ぐよう、技術は、デバイスデータへの無許可のアクセスを得ようとする試みが検出される場合に、復号化鍵が閉鎖されることを可能にする。実施において、復号化鍵は、様々な方法において、例えば、復号化鍵を削除すること、暗号化鍵をメモリに上書きすること、暗号化鍵を暗号化すること、等によって、閉鎖され得る。

【００１５】

実施形態は、閉鎖された復号化鍵がリカバリーエクスペリエンスを介して回復されることを可能にする。例えば、リカバリーエクスペリエンスは、ユーザに高度な認証情報を要求する認証プロシージャを含むことができる。そのような高度な認証情報は、権限のあるユーザによって取り出され得る高エントロピーのリカバリーパスワードを含むことができる。ユーザが正確なリカバリーパスワードを提供する場合に、リカバリーエクスペリエンスは、閉鎖された復号化鍵を回復させる、例えば、脱閉鎖させる、ことができる。実施に

おいて、閉鎖された復号化鍵が回復された後、ユーザは、デバイスログインエクスペリエンスの部分のような、デバイスへの標準の認証情報を提供することができる。認証が成功すると、回復された復号化鍵は、データがユーザ及び／又はデバイスの機能性によって“平文で”アクセスされ得るように、デバイスにおいてデータを復号するために使用され得る。

【００１６】

実施形態は、データに記憶されているデータを無許可のアクセスから保護するために使用され得るセキュリティポリシーを提供する。例えば、セキュリティポリシーは、特定の条件が存在する場合にデバイスのための復号化鍵が閉鎖されるべきであると特定することができる。そのような条件の例は、多数のデバイスログインの失敗、信頼できないデバイスにより暗号化されたデータにアクセスしようとする試み、復号化鍵及び／又は安全性に関連した信用証明物の明示的取り消し、特定の時点で“チェックイン”すべきデバイスの失敗、等に係ることができる。

【００１７】

１又はそれ以上の実施形態に従う実施例の概要が提示されているが、ここで、実施例が用いられ得る環境の例を考える。

【００１８】

環境の例

図１は、デバイスデータについてのセキュリティポリシーを提供する技術を用いるよう動作可能な実施例における環境１００の実例である。環境１００は、一例として制限なしに、デスクトップコンピュータ、ポータブルコンピュータ、パーソナルデジタルアシスタント（ＰＤＡ）のような手持ち式コンピュータ、携帯電話機、タブレットコンピュータ、及び同様のもののような、何らかの適切なコンピュータデバイスとして具現され得るクライアントデバイス１０２を含む。クライアントデバイス１０２の様々な異なる例は、図５において図示され以下で記載される。

【００１９】

図１のクライアントデバイス１０２は、クライアントデバイス１０２を介して様々なタスクを実行するための機能性を表すアプリケーション１０４を含むように表されている。そのようなタスクの例は、ウェブ検索、文書処理、電子メール、コンテンツ消費（例えば、映像及び／又は音声）、ソーシャルネットワーキング、等を含む。例えば、アプリケーション１０４は、ネットワーク１０６を介してナビゲーションするよう構成される機能性を表すウェブブラウザを含むことができる。ネットワーク１０６は、インターネット、ワイドエリアネットワーク（ＷＡＮ）、ローカルエリアネットワーク（ＬＡＮ）、無線ネットワーク、公衆電話網、イントラネット、等のような、多種多様の異なる構成を含み及び／又は前提としてよい。更に、単一のネットワーク１０６が示されているが、ネットワーク１０６は複数のネットワークを含むよう構成されてよい。アプリケーション１０４は、例えば、ネットワークリソースから入手できるコンテンツと相互作用し且つデータをネットワークリソースへ送る、例えば、ダウンロード及びアップロードを実行するように、ネットワーク１０６を介してナビゲーションするよう構成されてよい。

【００２０】

クライアントデバイス１０２の部分として更に、暗号化されたデータ１０８が表されている。データ１０８は、様々な異なるデータ暗号化技術を用いて暗号化され得る。暗号化されたデータ１０８は、例えば、クライアントデバイス１０２に存在する何らかの形態のコンピュータ可読記憶媒体に記憶され得る。そのようなコンピュータ可読記憶媒体の例は、図５を参照して以下で論じられる。実施において、暗号化されたデータ１０８は、コンテンツ（画像、映像、音声、等）、文書、連絡先、電子メール、等のようなユーザ及び／又は企業データを含むことができる。暗号化されたデータ１０８はまた、オペレーティングシステム（ＯＳ）データ、クライアントデバイス１０２のためのシステムファイル、アプリケーションファイル（例えば、実行ファイル）等のようなシステムデータを含むことができる。

【００２１】
クライアントデバイス１０２は、クライアントデバイス１０２のための様々な安全性に関連したタスクを管理及び／又は実行する機能性を表すセキュリティモジュール１１０を更に含む。例えば、セキュリティモジュール１１０は、データが暗号化されたデータ１０８の部分として記憶され得るように、クライアントデバイス１０２のためのデータを暗号化するよう構成され得る。様々なタイプのデータがセキュリティモジュール１１０によって暗号化され、暗号化されたデータ１０８の部分として含まれ得る。その例は先に与えられている。
【００２２】
セキュリティモジュール１１０は、暗号化されたデータ１０８を復号するために使用され得るデータの部分を表す少なくとも１つの復号化鍵１１２を含む。例えば、セキュリティモジュール１１０は、人によって認識される形態（例えば、人が読むことができる形態）、タスクを実行するためにアプリケーション１０４によって使用される形態、及び／又はシステムレベルの動作を実行する部分としてクライアントデバイス１０２によって用いられ得る形態にデータを置くために、暗号化されたデータ１０８を復号化鍵１１２を用いて復号することができる。
【００２３】
セキュリティモジュール１１０の部分として更に、セキュリティポリシー１１４が含まれる。セキュリティポリシー１１４は、セキュリティプロシージャをトリガすることができる条件及び／又は事象を表す。例えば、セキュリティモジュール１１０がセキュリティポリシー１１４の１つの違反を検出する場合に、セキュリティモジュール１１０は復号化鍵１１２を閉鎖させることができる。セキュリティポリシー１１４の例は、以下で詳細に論じられる。
【００２４】
セキュリティモジュール１１０は、クライアントデバイス１０２についての状態情報をモニタ及び／又はレポートする機能性を表すデバイスステータスモジュール１１６を更に含む。例えば、セキュリティポリシー１１４の１又はそれ以上は、クライアントデバイス１０２のための特定の状態条件を特定することができる。その特定の状態条件の変化がデバイスステータスモジュール１１６によって検出される場合に、デバイスステータスモジュール１１６は、セキュリティポリシー１１４の１つが違反されたとの通知を提供することができる。
【００２５】
例えば、デバイスステータスモジュール１１６は、プロセッサ、メモリ装置、入出力装置、等のような、クライアントデバイス１０２の様々な構成要素のための識別子を追跡することができる。よって、デバイスステータスモジュール１１６は、クライアントデバイス１０２のための既知の構成要素のプロファイルを保持することができる。デバイスステータスモジュール１１６が、未知の構成要素がクライアントデバイス１０２と相互作用しようと試みていると検出する場合に、デバイスステータスモジュール１１６は、セキュリティポリシー１１４の１つの違反をトリガすることができる。例えば、デバイスステータスモジュール１１６は、未知の中央演算処理装置（ＣＰＵ）又は信頼できないＣＰＵ構成がクライアントデバイス１０２に記憶されているデータ、例えば、暗号化されたデータ１０８にアクセスしようと試みていると検出することができる。これに応じて、セキュリティモジュール１１０は、未知のＣＰＵが復号化鍵１１２にアクセスして、暗号化されたデータ１０８を復号することを防ぐことができるように、復号化鍵１１２を閉鎖させることができる。他の状態に関連した情報の例は、以下で与えられる。
【００２６】
クライアントデバイス１０２の部分として更に、リカバリーモジュール１１８が含まれる。リカバリーモジュール１１８は、閉鎖されたセキュリティ鍵が回復されることを可能にする機能性を表す。例えば、復号化鍵１１２がセキュリティポリシー１１４の１つの違反に応答して閉鎖される場合に、リカバリーモジュール１１８は、復号化鍵１１２が回復

、例えば、脱閉鎖されること可能にすることができるリカバリープロシージャを開始することができる。リカバリープロシージャの詳細な例は、以下で論じられる。

【００２７】

環境１００は、エンティティのためのセキュリティプロシージャを管理及び／又は実行する機能性を表すセキュリティサービス１２０を更に含む。セキュリティサービス１２０は、ネットワーク１０６を介してクライアントデバイス１０２と通信することができる遠隔リソースによって実施され得る。例えば、セキュリティサービス１２０は、クライアントデバイス１０２のユーザに関連する企業エンティティ（例えば、ビジネス）のためのセキュリティプロシージャを管理することができる。セキュリティサービス１２０は、様々な項目についてのセキュリティステータスを追跡する少なくとも１つのセキュリティステータスリスト１２２を含む。例えば、セキュリティステータスリスト１２２は、クライアントデバイス、セキュリティ鍵、デジタル証明書、セキュリティ信用証明物、等のような特定の項目の信頼できるステータスが覆されたかどうかを特定することができる。

【００２８】

セキュリティサービス１２０は、例えば、クライアントデバイス１０２が権限のない個人に所有されている可能性があるとのインジケーションを受け取ることができる。例えば、クライアントデバイス１０２の権限のあるユーザは、クライアントデバイス１０２が紛失又は盗難されたことをセキュリティサービス１２０に知らせることができる。セキュリティサービス１２０は、クライアントデバイス１０２の信頼できるステータスを無効にさせることができ、これはセキュリティステータスリスト１２２に記録され得る。例えば、セキュリティサービス１２０は、復号化鍵１１２を無効にすることができ、これは、無効にされたとしてセキュリティステータスリスト１２２において印を付され得る。クライアントデバイス１０２がセキュリティサービス１２０にチェックインする場合に、クライアントデバイス１０２はセキュリティステータスリスト１２２にアクセスし、復号化鍵１１２が無効にされていることを検出することができる。これに応じて、セキュリティモジュール１１０は、復号化鍵１１２を閉鎖させることができる。代替的に、又は追加的に、セキュリティサービス１２０は、例えば、セキュリティステータスリスト１２２のコピーをクライアントデバイス１０２にプッシュすることによって、無効にされた項目の通知をクライアントデバイス１０２にプッシュすることができる。

【００２９】

本願で記載される技術が動作し得る例となる環境を記載してきたが、ここで、１又はそれ以上の実施形態に従う幾つかの例となるプロシージャの議論を考える。

【００３０】

プロシージャの例

下記の議論は、１又はそれ以上の実施形態に従ってデバイスデータのためのセキュリティポリシーを提供するプロシージャの例を記載する。下記の議論の部分において、図１の環境１００が参照される。

【００３１】

図２は、１又はそれ以上の実施形態に従う方法におけるステップを記載するフロー図である。実施において、方法は、セキュリティ鍵を保護するようデバイスを構成する方法の例を記載する。

【００３２】

ステップ２００は、デバイスについての暗号化されたデータを復号するために使用されるよう構成された復号化鍵を生成する。例えば、セキュリティモジュール１１０は、暗号化されたデータ１０８を復号するために使用され得る復号化鍵１１２を生成することができる。ステップ２０２は、復号化鍵が閉鎖されている場合に復号化鍵を回復するために使用され得るリカバリー鍵を生成する。例えば、復号化鍵は、セキュリティポリシーの違反に応答してそれを閉鎖するよう暗号化され得る。リカバリー鍵は、以下でより詳細に論じられるように、閉鎖された復号化鍵を回復するために用いられ得るリカバリープロシージャの部分として提供され得る。

【００３３】
図３は、１又はそれ以上の実施形態に従う方法におけるステップを記載するフロー図である。実施において、方法は、無許可のアクセスからデータを保護する方法の例を記載する。
【００３４】
ステップ３００は、デバイスについてのセキュリティポリシーの違反を検出する。例えば、セキュリティモジュール１１０は、セキュリティポリシー１１４の１又はそれ以上の違反を検出することができる。例となるセキュリティポリシーは、下記の項において論じられる。実施において、特定のセキュリティポリシーは、明記されたポリシーに基づかなくてよく、潜在的な安全上のリスクを引き起こすとの事象又は条件の解釈に基づいてよい。
【００３５】
ステップ３０２は、デバイスについての暗号化されたデータを復号するために使用されるよう構成されたセキュリティ鍵を閉鎖する。例えば、セキュリティモジュール１１０は、クライアントデバイス１０２についてのセキュリティポリシーの違反を検出することに応答して、復号化鍵１１２を閉鎖することができる。
【００３６】
実施において、セキュリティ鍵は、様々な異なる技術を用いて閉鎖され得る。例えば、セキュリティ鍵は、そのセキュリティ鍵を記憶するメモリの一部を消去及び／又は乱数値により上書きすることによって、閉鎖され得る。
【００３７】
代替的に、セキュリティ鍵は、例えば、中間のセキュリティ鍵を用いて、そのセキュリティ鍵を暗号化することによって、閉鎖され得る。よって、暗号化されたセキュリティ鍵を回復するよう、ユーザは、中間のセキュリティ鍵及び／又は中間のセキュリティ鍵に関連する秘密鍵を提供することができる。例えば、ユーザは、何らかの形態の入力メカニズムを用いて中間のセキュリティ鍵を入力してよい。代替的に、又は追加的に、ユーザは、中間のセキュリティ鍵が取り出され得る遠隔の及び／又は保護された記憶位置のような、どこに中間のセキュリティ鍵が置かれているのかのインジケーションを提供してよい。例えば、中間のセキュリティ鍵はセキュリティサービス１２０によって記憶されてよい。リカバリープロシージャが暗号化されたセキュリティ鍵を回復するのに成功するよう実行される場合に、中間のセキュリティ鍵は、セキュリティサービス１２０からクライアントデバイス１０２によって取り出され、暗号化されたセキュリティ鍵を復号するために使用され得る。
【００３８】
多数の異なる変形例は、閉鎖されたセキュリティ鍵が権限のないエンティティによって取り出され得ないことを確かにするために用いられ得る。例えば、セキュリティ鍵を記憶するメモリの一部分は、セキュリティポリシーの違反のインジケーションに応答して、ランダムデータにより（例えば、複数回）上書きされ得る。これは、メモリのその部分に書き込まれているセキュリティ鍵値を更に不明瞭に又は閉鎖する働きをすることができる。
【００３９】
他の変形例として、セキュリティ鍵は、セクション（例えば、スプリット）に分割可能であり、セクションの夫々は、メモリの別個の部分（例えば、セクタ）に記憶され得る。よって、消去又は上書き動作がメモリの一部分において失敗する場合に、セキュリティ鍵の他の部分はメモリの他の部分において消去及び／又は上書き可能である。例えば、メモリセクタの不具合によりセキュリティ鍵の片を記憶するメモリの一部分が消去又は上書きされることを妨げられる場合に、他のメモリセクタは依然として、セキュリティ鍵の全ての部分が権限のないエンティティへ露わにされることを防ぐよう消去及び／又は上書きされ得る。
【００４０】
ステップ３０４は、閉鎖されたセキュリティ鍵のためのリカバリープロシージャを開始

する。例えば、リカバリーモジュール１１８は、復号化鍵１１２が閉鎖された後に回復されることを可能にすることができるリカバリープロシージャを起動することができる。例となるリカバリープロシージャは以下で詳細に論じられる。

【００４１】

少なくとも幾つかの実施形態において、セキュリティ鍵閉鎖プロシージャを実施するより前に、リカバリー鍵が少なくとも１つの外部位置（例えば、クライアントデバイス１０２の外部）に永続されるかどうかが決定される。セキュリティ鍵が他の位置に永続されているかどうかが決定され得ない場合は、幾つかの実施は、セキュリティ鍵を閉鎖することを回避する。例えば、クライアントデバイスは、最初の認証（例えば、ログオン）モードのままであってよい。

【００４２】

図４は、１又はそれ以上の実施形態に従う方法におけるステップを記載するフロー図である。実施において、方法は、図３を参照して上述された方法のステップ３０４を実行する詳細な方法を記載する。

【００４３】

ステップ４００は、セキュリティ鍵が閉鎖されたことに応答して、デバイスリブートを開始する。例えば、セキュリティモジュール１１０は、復号化鍵１１２がセキュリティポリシーの１つの違反に基づき閉鎖されたことに応答して、クライアントデバイス１０２のリブートを開始することができる。

【００４４】

ステップ４０２は、デバイスのためのオペレーティングシステムデータが利用可能でないことを検出する。例えば、クライアントデバイス１０２のためのオペレーティングシステム（ＯＳ）データは、暗号化されたデータ１０８の部分のように、暗号化された形において記憶され得る。よって、復号化鍵１１２が閉鎖されない典型的な機能シナリオにおいて、ＯＳデータは、記憶部から読み出され、復号化鍵１１２により復号され得る。復号されたＯＳデータは、次いで、クライアントデバイス１０２がクライアントデバイス１０２のための様々なタスクを実行することを可能にするよう、クライアントデバイス１０２をブートする部分として（例えば、主メモリに）ロードされ得る。復号化鍵１１２が閉鎖されているシナリオでは、しかしながら、ＯＳデータは復号化及びロードされ得ない。

【００４５】

ステップ４０４は、リカバリー鍵を要求するデバイスリカバリーエクスペリエンスを起動する。例えば、クライアントデバイス１０２のためのブートローダは、ＯＳデータが利用可能でないことを検出することができ、そして、リカバリーモジュール１１８にリカバリーエクスペリエンスを開始するよう通知することができる。リカバリーモジュール１１８は、クライアントデバイス１０２を介して表示され且つユーザにリカバリー鍵を提供するよう促すグラフィカルユーザインターフェース（ＧＵＩ）のような、リカバリー鍵のためのプロンプトを提供することができる。実施において、リカバリーモジュール１１８は、平文で（例えば、暗号化されずに）クライアントデバイス１０２に記憶され、それにより、デバイスリカバリーエクスペリエンスは、復号化鍵１１２が閉鎖される事象において起動され得る。例えば、リカバリーモジュール１１８は、クライアントデバイス１０２においてファームウェアで実装され得る。

【００４６】

実施において、リカバリー鍵は、クライアントデバイス１０２のユーザによってアクセスされ得るがクライアントデバイス１０２に容易に利用可能でない情報を含む。例えば、リカバリー鍵は、クライアントデバイス１０２に記憶されない長い（例えば、４８文字以上）高エントロピーパスワードであり得る。代替的に、又は追加的に、リカバリー鍵は、生体認証、スマートカード認証、無線周波数識別（ＲＦＩＤ）装置を介するＲＦＩＤ、チャレンジ問題への解答等のような他の形態の認証を含むことができる。

【００４７】

他の例として、リカバリー鍵は、別個の認証エクスペリエンスの部分としてアクセスさ

れ得る。例えば、ユーザは、別個のパスワード及び／又は他の認証ファクタをセキュリティサービス１２０へ提供することができる。認証ファクタが正しい場合は、ユーザはリカバリー鍵を提供され得、且つ／あるいは、リカバリー鍵は自動的にセキュリティサービス１２０からクライアントデバイス１０２へ送られ得る。更なる他の例として、リカバリー鍵は、システムアドミニストレータ、情報技術（ＩＴ）要員、等のような、デバイスに関連する企業職員によって取り出されてよい。

【００４８】

ステップ４０６は、正しいリカバリー鍵が提供されるかどうかを決定する。正しいリカバリー鍵が提供される場合は、ステップ４０８は、復号化鍵が回復されることを可能にする。例えば、クライアントデバイス１０２は、標準のパスワードのようなログオン情報を要求する標準のデバイスログオンエクスペリエンスにリブートされ得る。実施において、標準のパスワードは、低エントロピーパスワードを指すことがある。例えば、標準のパスワードは、デバイスを解除するために使用され得る４桁の個人識別番号（ＰＩＮ）であり得る。ユーザが復号化鍵１１２の回復に成功する場合に、クライアントデバイス１０２はブートされ、復号化鍵１１２は暗号化されたデータ１０８を復号するために使用され得る。代替的に、又は追加的に、ログオンエクスペリエンスはリカバリーエクスペリエンスに組み込まれてよい。

【００４９】

実施において、閉鎖されているセキュリティ鍵を回復することは、如何にしてセキュリティ鍵が閉鎖されたかに基づくことができる。例えば、セキュリティ鍵がメモリにおいて消去及び／又は上書きされることで閉鎖された場合は、セキュリティ鍵は遠隔のリソース、例えば、セキュリティサービス１２０から取り出され得る。代替的に、セキュリティ鍵が中間のセキュリティ鍵により暗号化された場合は、中間のセキュリティ鍵が取り出され、セキュリティ鍵を復号するために使用され得る。

【００５０】

ステップ４０６に戻って、正しいリカバリー鍵が提供されない場合は、ステップ４１０は、復号化鍵が回復されないようにする。例えば、クライアントデバイス１０２は、リカバリーエクスペリエンスモードのままで正しいリカバリー鍵を待つことができる。代替的に、又は追加的に、正しいリカバリー鍵を提供する閾回数の試みが失敗する場合は、クライアントデバイス１０２は、クライアントデバイス１０２に記憶されているデータの一部又は全てを消去及び／又は上書きするメモリワイプを生じさせることができる。これは復号化鍵１１２を消去することを含んでよい。

【００５１】

上記のリカバリープロシージャへの代替の実施として、復号化鍵は、クライアントデバイスから遠隔にあるリソースから取り出されてよい。例えば、復号化鍵は、システムアドミニストレータ、情報技術（ＩＴ）要員等のような、クライアントデバイスに関連する企業職員によってセキュリティサービス１２０から取り出されてよい。

【００５２】

幾つかの例となるプロシージャを論じてきたが、ここで、１又はそれ以上の実施形態に従う幾つかの例となるセキュリティポリシーの議論を考える。

【００５３】

セキュリティポリシー

様々な異なるセキュリティポリシーが、デバイスに関連するデータを無許可のアクセスから保護するために用いられ得る。例えば、セキュリティポリシーは、デバイス認証状態、デバイスハードウェア状態、デバイス接続ステータス、等のような、多数の異なるデバイスに関連する考慮すべき事柄に基づくことができる。以下では、例えば、上記のセキュリティポリシー１１４の部分として、１又はそれ以上の実施形態に従って実施され得る幾つかの例となるセキュリティポリシーが論じられる。更に、セキュリティポリシーは、全体として又は部分的に、クライアントデバイス１０２によって遠隔のリソースから独立して施行され得る。例となるセキュリティポリシーは、請求される実施形態に制限するよう

意図されず、単に例示のために与えられる。

【００５４】

認証の失敗

実施において、デバイスは、ユーザがそのデバイスのデータ及び機能性にアクセスすることを可能にするログオンプロシージャを用いることができる。例えば、デバイスが起動され及び／又はハイバネーションモードから起きる場合に、ログオンプロンプトが提示され、パスワード又は他の認証ファクタを要求する。ユーザが正しい認証ファクタを提供する場合は、ユーザは、デバイスのデータ及び機能性にアクセスすることを認められ得る。例えば、クライアントデバイス１０２を参照して、正しい認証ファクタを提供することは、暗号化されたデータ１０８が復号され利用され得るように、復号化鍵１１２へのアクセスを可能にし及び／又はその継続的な使用を認めることができる。

【００５５】

しかしながら、ユーザが正しい認証ファクタを提供することができない場合は、デバイスはデータ及び／又は機能性へのアクセスをブロックすることができる。例えば、正しい認証ファクタを提供することの失敗は、デバイスをログオンエクスペリエンスにとどまらせることができ、それにより、そのデバイスのデータ及び他の機能性は、正しい認証ファクタが提供されない限りは利用可能でない。

【００５６】

実施において、デバイスに関連するログオンの失敗回数に基づくセキュリティポリシーが用いられ得る。例えば、デバイスのための失敗したログオン試行の閾回数は予め指定され得る。実際のログオン失敗回数が閾回数（例えば、５回の失敗したログオン試行）に達し及び／又は超える場合は、デバイスは、更なるログオン試行が不可能にされ且つセキュリティポリシーの違反がトリガされるように、ロックされ得る。例えば、クライアントデバイス１０２を参照して、セキュリティモジュール１１０は、復号化鍵１１２を閉鎖させることができる。更に、リカバリーモジュール１１８は、上述されたようにリカバリープロシージャを開始することができる。少なくとも幾つかの実施形態において、ログオン試行の閾回数は設定可能である。例えば、ユーザ、ネットワークアドミニストレータ、ＩＴ要員等のような様々な異なるエンティティが閾回数を指定することができる。

【００５７】

ログオンの失敗回数を追跡する場合に、実施形態は、ログオン失敗の総数の部分として様々な異なるログオン技術を考慮することができる。例えば、個人が正しいパスワードを提供し且つ正しい親指の指紋を提供することができず、更にはチャレンジ問題に正確に応答することができない場合に、それらは３回の失敗したログオン試行としてカウントされ得る。よって、ログオンの失敗回数は、異なるログオン技術及び／又は認証ファクタに基づき累積的であり得る。更に、失敗したログオン試行は、複数の異なるユーザからのログオン試行に基づくことができる。

【００５８】

そのようなセキュリティポリシーを実装することは、権限のないユーザがデバイスのデータ及び／又は機能性への無許可のアクセスを得ようとする試みにおいて繰り返しパスワードを推測し及び／又は異なる認証ファクタを提供することを妨げることができる。

【００５９】

信頼できるステータスの取り消し

実施において、セキュリティポリシーは、デバイスに関する項目の信頼できるステータスが無効にされ得ることを特定することができる。そのようなデバイスに関する項目の例は、デバイス自体、デバイスによって使用されるデジタル証明書、デバイスに関連するセキュリティ鍵、セキュリティ信用証明物、等を含む。

【００６０】

実施例において、セキュリティポリシーは、クライアントデバイス１０２が、セキュリティステータスリスト１２２でリストアップされている項目のリボケーションステータスのようなリボケーション情報をセキュリティサービス１２０に定期的にクエリすべきこと

を特定することができる。リボケーション情報が、クライアントデバイス１０２の信頼できるステータスが無効にされていることを示す場合は、復号化鍵１１２は閉鎖され、リカバリープロシージャが開始され得る。上述されたように、デバイスの信頼できるステータスは、そのデバイスが紛失又は盗難されたことをユーザが示すことに応答して、無効にされ得る。追加的に、又は代替的に、信頼できるステータスは、セキュリティ鍵、デジタル証明書、及び／又は他のセキュリティに関する項目が危うくされたとのインジケーションに基づき、無効にされ得る。

【００６１】

デバイスがハイバネーション及び／又はスリープモードに入ることができる実施において、デバイスは、リボケーション情報をクエリするよう、そのようなモードから自動的に浮上（例えば、起動）するよう構成され得る。例えば、リボケーションインターバル（例えば、４時間ごと）が特定され得、その後に、デバイスは、リボケーション情報をクエリすべきである。デバイスがスリープモードにある間にリボケーションインターバルが経過する場合は、デバイスは、自動的に目覚め、リボケーション情報をクエリすることができる。よって、技術は、様々なエンティティがデバイスの信頼できるステータスをモニタし、デバイスの信頼できるステータスを無効にして無許可のアクセスからデバイスを保護することを可能にする。

【００６２】

少なくとも幾つかの実施形態において、リボケーション情報は、遠隔リソースからクライアントデバイスへプッシュされ得る。例えば、セキュリティサービス１２０は、例えば、通知の部分として、リボケーションデータをクライアントデバイス１０２へプッシュすることができる。代替的に、又は追加的に、遠隔リソースは、セキュリティ鍵を閉鎖するプロシージャを開始するようデバイスの機能性にアクセスすることができる。例えば、セキュリティサービス１２０は、セキュリティポリシー１１４の１つが違反されたことを検出することができる。これに応じて、セキュリティサービス１２０は、（例えば、信頼できるデジタル証明書に基づき）信頼できるエンティティとしてセキュリティモジュール１１０と通信し、セキュリティモジュール１１０に復号化鍵１１２を閉鎖するよう促すことができる。よって、実施は、クライアントデバイスが、リボケーション情報のためのクライアントデバイスによるクエリとは無関係に、リボケーション情報を受信することを可能にすることができる。

【００６３】

強制チェックイン

実施において、デバイスがチェックインしない場合に、そのデバイスに関連するセキュリティ鍵が自動的に閉鎖されるべきであることを特定するセキュリティポリシーが、用いられ得る。例えば、セキュリティモジュール１１０は、例えば、リボケーション情報をクエリするために及び／又はデバイスが現在信頼できる状態にあることを確認するために、セキュリティサービス１２０に定期的にチェックインするよう構成される。セキュリティモジュール１１０が、チェックインインターバルが経過した後にチェックインしようと試み、セキュリティサービス１２０とコンタクトをとることができない場合は、セキュリティモジュール１１０はセキュリティポリシー違反をトリガすることができる。例えば、セキュリティモジュール１１０は、デバイスデータがアクセスされ得ないように、復号化鍵１１２を閉鎖し且つ／あるいはデバイスをロックすることができる。

【００６４】

そのようなチェックインプロシージャを用いることは、デバイスがネットワーク接続を失っており、よって遠隔のサービスと通信してリボケーション情報をチェックすることができないシナリオにおいて、データが安全なままであることを可能にすることができる。そのようなシナリオは、権限のないユーザがデバイスを取得し、デバイスが、例えば、デバイスのネットワーク通信機能性を無効にすることによって、遠隔リソースと通信することを妨げる場合に、起こり得る。

【００６５】

デバイス状態
実施において、特定のデバイス状態条件において変化が起こる場合に、セキュリティポリシーが違反されていることを特定するセキュリティポリシーが、用いられ得る。例となるデバイス状態条件は、ハードウェア状態、ソフトウェア状態、ネットワーク状態、等を含む。
【００６６】
ハードウェア状態を参照して、ハードウェア識別子は、デバイスの様々な既知のハードウェア部品について記録されモニタされ得る。未知のハードウェアが（例えば、デバイスデータを取得するために）デバイスと交信しようと試みる場合は、セキュリティプロシージャの違反の通知が生成され得る。例えば、権限のないユーザがクライアントデバイス１０２からデータ記憶装置を取り外し、そのデータ記憶装置を別のデバイスに接続することがある。権限のないユーザは、例えば、別のデバイスを用いてデータ記憶装置からデバイスデータにアクセスするよう試みることがある。デバイスステータスモジュール１１６は、データ記憶装置に記憶され得、未知のデバイスがデータ記憶装置と交信していることを検出することができる。デバイスステータスモジュール１１６は、未知のデバイスをセキュリティモジュール１１０に通知することができ、これにより、復号化鍵１１２は、権限のないユーザが復号化鍵１１２にアクセスして暗号化されたデータ１０８を復号することを防ぐよう閉鎖され得る。
【００６７】
ソフトウェア状態は、様々なソフトウェアに関する条件を含むことができる。例えば、ソフトウェア状態は、アプリケーションにインストールされるパッチのインジケーションのような、アプリケーションの更新ステータスを含むことができる。実施において、アプリケーションのセキュリティ脆弱性を修正することができるパッチが（例えば、アプリケーション開発者から）アプリケーションに利用可能であり得る。よって、利用可能なパッチがアプリケーションにインストールされていないと決定される場合は、デバイスステータスモジュール１１６は、起こり得る安全上のリスクにクライアントデバイス１０２をさらさないようセキュリティポリシー違反をトリガすることができる。
【００６８】
他のソフトウェア状態は、ソフトウェアの特定の部分の信頼できるステータスに関係があり得る。ソフトウェアが（例えば、セキュリティステータスリスト１２２において）信頼できないと示される場合は、セキュリティポリシーの違反がトリガされ得る。
【００６９】
更なるソフトウェア状態は、健全な作動環境を示すと特定される推奨ソフトウェアを参照することができる。例えば、セキュリティに関するソフトウェア（例えば、ウィルス対策ソフトウェア）は、マルウェアがデバイスに存在しないことを確認するために用いられ得る。推奨ソフトウェアが存在せず且つ／あるいはデバイスで実行されていない場合は、セキュリティポリシー違反がトリガされ得る。
【００７０】
ネットワーク状態は、デバイスが接続される特定のネットワーク、デバイスがアクセスしているネットワークリソース（例えば、ウェブサイト）、等のような、様々なネットワークに関する条件を参照することができる。危険なネットワーク条件が検出される場合は、セキュリティポリシーの違反がトリガされ得る。例えば、デバイスステータスモジュール１１６が、クライアントデバイス１０２が信頼できないサーバ及び／又は信頼できないウェブサイトと通信していることを検出する場合は、デバイスステータスモジュール１１６は、セキュリティポリシー違反をトリガすることができる。
【００７１】
時間クロックステータス
実施において、時間に関する変化が起こる場合に、セキュリティポリシーが違反されたと特定するセキュリティポリシーが、用いられ得る。例えば、権限のないユーザが、実デバイス時間のような、デバイスに関連する時間パラメータを変更しようと試みることがあ

る。権限のないユーザは、例えば、特定のセキュリティに関する事象をトリガすることを無効にするためにデバイス時間を後退させようと試みることがある。上記の定期的なデバイスチェックインを参照して、権限のないユーザは、チェックインインターバルが経過した後にデバイスにチェックインすることができない場合に起こり得るセキュリティポリシー違反をトリガすることを無効にするために、時間の後退を実施しようと試みるかもしれない。

【００７２】

よって、実施は、時間に関する変化をモニタする時間確認メカニズムを用いることができる。例えば、時間クロックは、例えば、クライアントデバイスにある信頼できるハードウェア及び／又はファームウェアにおいて、信頼できる時間装置として実装され得る。信頼できる時間装置は、例えば、トラステッド・プラットフォーム・モジュール（Trusted Platform Module）（ＴＰＭ）装置として実装され得る。時間クロックが期待されるように機能していないことが検出される場合は、セキュリティポリシー違反がトリガされ得る。例えば、不調の時間クロックは、デバイス時間及び／又は他の時間パラメータを変更しようとする試みにおける権限のないエンティティによる起こり得る改ざんのインジケーションであり得る。よって、潜在的な時間クロックの改ざんが検出される場合は、セキュリティポリシー違反がトリガされ得る。

【００７３】

地理的な位置

実施において、デバイスについての地理的なパラメータを特定するセキュリティポリシーが用いられ得る。例えば、クライアントデバイスは、クライアントデバイスの地理的な位置を決定する機能性を用いることができる。そのような機能性の例は、グローバル・ポジショニング・システム（global positioning system）（ＧＰＳ）機能性、携帯電話三角測量機能性、ネットワークベースの位置決め、等を含む。

【００７４】

地理的セキュリティポリシーは、デバイスが特定の地理的範囲の外にある場合は、セキュリティポリシーが違反されていると特定することができる。例えば、企業エンティティは、設備資産の周りの定義された範囲のような、エンティティに関連する地理的範囲を定義することができる。クライアントデバイスが定義された地理的範囲の外で検出される場合は、セキュリティポリシーの違反がトリガされ得る。更に、地理的な位置情報を得ようとする試みが、例えば、デバイスの位置決め機能性が無効にされていることにより、失敗することがある。実施において、クライアントデバイスが地理的な位置情報を取得することができない場合は、セキュリティポリシーの違反がトリガされ得る。

【００７５】

他の例として、例えば、信頼できないエンティティに関連するような、特定の地理的領域は危険と特定され得る。デバイスが危険な地理的領域内にあると決定される場合は、セキュリティポリシーの違反がトリガされ得る。このように、セキュリティポリシーは、デバイスについて、デバイスの位置に基づきデバイスデータへのアクセスを制御するよう特定され得る。

【００７６】

幾つかの例となるセキュリティポリシーについて論じてきたが、ここで、１又はそれ以上の実施形態に従う幾つかの実施変形例の議論を考える。

【００７７】

実施変形例

ここで論じられている実施に対する多数の異なる変形例は、１又はそれ以上の実施形態に従って用いられ得る。

【００７８】

ハードウェアベースのセキュリティ

実施において、様々なセキュリティプロシージャは、無許可のアクセスからデータを保護するようハードウェア内で実施され得る。例えば、クライアントデバイスに関連するデ

ータ記憶装置は、デバイス自体でデータの暗号化及び復号化を行うよう構成され得る。そのような実施において、データ記憶装置は、データ記憶装置自体で復号化鍵を記憶し利用することができる。データ記憶装置は内部で復号化を実行するので、データ記憶装置は、クライアントデバイスのＯＳのような他の構成要素へ復号化鍵を解放する必要がない。よって、権限のないユーザがデータ記憶装置から復号化鍵にアクセスしようとする場合に、データ記憶装置は、ホストクライアントデバイスで実行中のソフトウェアと無関係に復号化鍵を閉鎖することができる。

【００７９】

自動閉鎖

実施において、セキュリティ鍵は、様々な事象に応答して自動的に閉鎖され得る。例えば、デバイスが特定のモードに入る場合に、デバイスのための暗号化鍵がこれに応答して閉鎖され得る。そのようなモードの例は、ロックモード、スリープモード、ハイバネーションモード、等を含む。実施において、デバイスは、デバイスがロックモードに入ることを要求する入力を提供することといったユーザ動作に応答して、ロックモードに入ることができる。

【００８０】

デバイスがそのようなモードから現れた後に、閉鎖されている暗号化鍵を回復するよう、デバイスは、その状態を確認するよう遠隔リソースと通信することができる。例えば、クライアントデバイス１０２がそのようなモードから現れる場合に、セキュリティモジュール１１０は、クライアントデバイス１０２のセキュリティステータスをセキュリティサービス１２０にクエリすることができる。セキュリティステータスが、クライアントデバイス１０２の信頼できるステータスが無効にされていないことを示す場合は、復号化鍵１１２はクライアントデバイス１０２にリストアされ得る。そうではなく、クライアントデバイス１０２の信頼できるステータスが無効にされており且つ／あるいは試みられたセキュリティサービス１２０への接続が失敗する場合は、クライアントデバイス１０２はリカバリープロシージャを起動することができる。例となるリカバリープロシージャは、先に論じられている。

【００８１】

幾つかの例となる実施変形例について論じてきたが、ここで、１又はそれ以上の実施形態に従う例となるシステム及びデバイスの議論を考える。

【００８２】

例となるシステム及びデバイス

図５は、ここで記載される様々な技術を実施し得る１以上のコンピュータシステム及び／又は装置を表す例となるコンピュータデバイス５０２を含むシステムの例を全体として５００で表す。例えば、図１を参照して上述されたクライアントデバイス１０２は、コンピュータデバイス５０２として具現され得る。コンピュータデバイス５０２は、例えば、サービスプロバイダのサーバ、クライアントに関連するデバイス（例えば、クライアントデバイス）、オンチップのシステム、及び／又は何らかの他の適切なコンピュータデバイス若しくはコンピュータシステムであってよい。

【００８３】

表されている例となるコンピュータデバイス５０２は、互いに通信上結合されているプロセッシングシステム５０４、１以上のコンピュータ可読媒体５０６、及び１以上の入出力（Ｉ／Ｏ）インターフェース５０８を有する。図示されていないが、コンピュータデバイス５０２は、様々な構成要素を互いに結合するシステムバス又は他のデータ及びコマンド伝送システムを更に有してよい。システムバスは、様々なバスアーキテクチャのいずれかを利用するメモリバス若しくはメモリコントローラ、ペリフェラルバス、ユニバーサルシリアルバス、及び／又はプロセッサ若しくはローカルバスのような、異なるバス構造のうちのいずれか１つ又は組み合わせを含むことができる。制御及びデータラインのような、様々な他の例も考えられる。

【００８４】

プロセッシングシステム５０４は、ハードウェアを用いて１以上の動作を実行する機能性を表す。加えて、プロセッシングシステム５０４は、プロセッサ、機能ブロック、等として構成され得るハードウェア要素５１０を含むように表されている。これは、１以上の半導体を用いて形成された特定用途向け集積回路又は他のロジックデバイスとしてのハードウェアにおける実施を含んでよい。ハードウェア要素５１０は、それらが形成される材料又はそれらで用いられる処理メカニズムによって制限されない。例えば、プロセッサは、半導体及び／又はトランジスタ（例えば、電子集積回路（ＩＣ））から成ってよい。そのような状況において、プロセッサにより実行可能な命令は、電子的に実行可能な命令であってよい。

【００８５】

コンピュータ可読媒体５０６は、メモリ／ストレージ５１２を含むように表されている。メモリ／ストレージ５１２は、１以上のコンピュータ可読媒体に関連するメモリ／ストレージ容量を表す。メモリ／ストレージ５１２は、揮発性媒体（例えば、ランダムアクセスメモリ（ＲＡＭ））及び／又は不揮発性媒体（例えば、読み出し専用メモリ（ＲＯＭ）、フラッシュメモリ、光ディスク、磁気ディスク、等）を含んでよい。メモリ／ストレージ５１２は、固定媒体（例えば、ＲＡＭ、ＲＯＭ、固定ハードドライブ、等）及びリムーバブル媒体（例えば、フラッシュメモリ、リムーバブルハードドライブ、光ディスク、等）を含んでよい。コンピュータ可読媒体５０６は、以下で更に記載されるように様々な他の方法において構成されてよい。

【００８６】

入出力インターフェース５０８は、様々な入出力装置を用いて、ユーザがコンピュータデバイス５０２にコマンド及び情報を入力することを可能にし、更には、情報がユーザ及び／又は他の構成要素若しくはデバイスに提示されることを可能にする機能性を表す。入力装置の例は、キーボード、カーソル制御装置（例えば、マウス）、マイクロホン（例えば、音声認識及び／又は音声入力用）、スキャナ、タッチ機能性（例えば、物理的な接触を検出するよう構成される容量性又は他のセンサ）、カメラ（例えば、接触を伴わない動きをジェスチャとして検出するために赤外線周波数のような可視又は不可視の波長を用いてよい。）、等を含む。出力装置の例は、表示装置（例えば、モニタ又はプロジェクタ）、スピーカ、プリンタ、ネットワークカード、触覚応答装置、等を含む。よって、コンピュータデバイス５０２は、ユーザインタラクションをサポートするよう、以下で更に記載されるように様々な方法において構成されてよい。

【００８７】

様々な技術は、ソフトウェア、ハードウェア要素、又はプログラムモジュールの一般情勢においてここで記載され得る。概して、そのようなモジュールは、特定のタスクを実行し又は特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、エレメント、コンポーネント、データ構造、等を含む。ここで使用される語「モジュール」、「機能性」、及び「コンポーネント」は、概して、ソフトウェア、ファームウェア、ハードウェア、又はそれらの組み合わせを表す。ここで記載される技術の特徴は、プラットフォーム非依存であり、これは、技術が、様々なプロセッサを備える様々な市販のコンピュータプラットフォームにおいて実施され得ることを意味する。

【００８８】

記載されるモジュール及び技術の実施は、何らかの形態のコンピュータ可読媒体に記憶され又はそれを介して伝送されてよい。コンピュータ可読媒体は、コンピュータデバイス５０２によってアクセスされ得る様々な媒体を含んでよい。例として、制限なしに、コンピュータ可読媒体は、「コンピュータ可読記憶媒体」及び「コンピュータ可読信号媒体」を含んでよい。

【００８９】

「コンピュータ可読記憶媒体」は、単なる信号伝送、搬送波、又は信号自体と対照的に、情報の永続的及び／又は非一時的な記憶を可能にする媒体及び／又は装置を指すことができる。よって、コンピュータ可読記憶媒体は、信号担持媒体（signal bearing mediu

m）を含まない。コンピュータ可読記憶媒体は、コンピュータ可読命令、データ構造、プログラムモジュール、ロジック要素／回路、又は他のデータのような情報の記憶に適した方法又は技術において実施される揮発性及び不揮発性のリムーバブル及び非リムーバブルな媒体及び／又は記憶装置のようなハードウェアを含む。コンピュータ可読記憶媒体の例は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリ若しくは他のメモリ技術、ＣＤ－ＲＯＭ、デジタルバーサタイルディスク（ＤＶＤ）若しくは他の光学記憶装置、ハードディスク、磁気カセット、磁気テープ、磁気ディスク記憶装置若しくは他の磁気記憶装置、又は他の記憶装置、有形的媒体、あるいは、所望の情報を記憶するのに適し且つコンピュータによってアクセスされ得る製品を含んでよいが、これらに限られない。

【００９０】

「コンピュータ可読信号媒体」は、例えば、ネットワークを介して、コンピュータデバイス５０２のハードウェアへ命令を送信するよう構成される信号担持媒体を指すことができる。信号媒体は、通常は、コンピュータ可読命令、データ構造、プログラムモジュール、又は他のデータを、搬送波、データ信号、又は他のトランスポートメカニズムのような変調データ信号において具現してよい。信号媒体はまた、あらゆる情報配信媒体を含む。語「変調データ信号」は、信号において情報を符号化するような態様において変更されたその特性セットの１以上を有する信号を意味する。例として、制限なしに、通信媒体は、有線ネットワーク又は直接配線接続のような有線媒体と、音響、無線周波数（ＲＦ）、赤外線、及び他の無線媒体のような無線媒体とを含む。

【００９１】

上述されたように、ハードウェア要素５１０及びコンピュータ可読媒体５０６は、ここで記載される技術の少なくとも幾つかの態様を実施するよう幾つかの実施形態において用いられ得るハードウェアにおいて実施される命令、モジュール、プログラム可能なデバイスロジック及び／又は固定デバイスロジックを表す。ハードウェア要素は、集積回路若しくはオンチップのシステム、特定用途向け集積回路（ＡＳＩＣ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、コンプレックスプログラマブルロジックデバイス（ＣＰＬＤ）、及びシリコン又は他のハードウェアデバイスにおける他の実施の構成要素を含んでよい。これに関連して、ハードウェア要素は、例えば、上記のコンピュータ可読記憶媒体のような、実行のための命令を記憶するのに利用されるハードウェアデバイス及びハードウェア要素によって具現される命令、モジュール、及び／又はロジックによって定義されるプログラムタスクを実行するプロセッシング装置として動作してよい。

【００９２】

上記の組み合わせはまた、ここで記載される様々な技術及びモジュールを実施するために用いられてよい。然るに、ソフトウェア、ハードウェア、又はプログラムモジュール及び他のプログラムモジュールは、１以上のハードウェア要素５１０によって及び／又は何らかの形態のコンピュータ可読記憶媒体において具現される１以上の命令及び／又はロジックとして実施されてよい。コンピュータデバイス５０２は、ソフトウェア及び／又はハードウェアモジュールに対応する特定の命令及び／又は機能を実施するよう構成されてよい。然るに、ソフトウェアとしてコンピュータデバイス５０２によって実行可能であるモジュールの実施は、例えば、プロセッシングシステムのハードウェア要素５１０及び／又はコンピュータ可読記憶媒体の使用を通じて、少なくとも部分的にハードウェアにおいて達成されてよい。命令及び／又は機能は、ここで記載される技術、モジュール、及び例を実施するよう１以上の製品（例えば、１以上のコンピュータデバイス５０２及び／又はプロセッシングシステム５０４）によって実行可能／動作可能であってよい。

【００９３】

図５に更に表されるように、例となるシステム５００は、パーソナルコンピュータ（ＰＣ）、テレビ受像機、及び／又はモバイル機器においてアプリケーションを実行する場合に、シームレスなユーザエクスペリエンスのためのユビキタス環境を可能にする。サービス及びアプリケーションは、アプリケーションを利用しながら、ビデオゲームで遊びながら、ビデオを見ながら、等の最中に１つのデバイスから次のデバイスへ移動する場合に、

共通のユーザエクスペリエンスのために、３つ全ての環境において実質的に同じように実行される。

【００９４】

例となるシステム５００において、複数のデバイスは、中央コンピュータデバイスを通じて相互接続される。中央コンピューティングデバイスは、複数のデバイスにとって局在的であってよく、あるいは、複数のデバイスから遠く離れて設置されてよい。一実施形態において、中央コンピュータデバイスは、ネットワーク、インターネット、又は他のデータ通信リンクを通じて複数のデバイスへ接続される１以上のサーバコンピュータのクラウドであってよい。

【００９５】

一実施形態において、この相互接続アーキテクチャは、複数のデバイスにわたって提供される機能性がそれら複数のデバイスのユーザに共通したシームレスなエクスペリエンスを与えることを可能にする。複数のデバイスの夫々は、異なる物理的な要件及び機能を備えてよく、中央コンピュータデバイスは、各デバイスへ合わせられていながら全てのデバイスに共通であるエクスペリエンスのデバイスへの提供を可能にするプラットフォームを使用する。一実施形態において、標的デバイスの分類が生成され、エクスペリエンスはデバイスの汎用分類に合わせられる。デバイスの分類は、デバイスの物理的な特性、使用形態、又は他の共通の特性によって定義されてよい。

【００９６】

様々な実施において、コンピュータデバイス５０２は、例えば、コンピュータ５１４、モバイル５１６、及びテレビジョン５１８の使用のために、様々な異なる構成を仮定してよい。それらの構成の夫々は、概して異なる構成及び機能を備えうるデバイスを含み、よって、コンピュータデバイス５０２は、異なるデバイス分類のうちの１以上に従って構成されてよい。例えば、コンピュータデバイス５０２は、パーソナルコンピュータ、デスクトップコンピュータ、マルチスクリーンコンピュータ、ラップトップコンピュータ、ネットブック等を含むデバイスのコンピュータ５１４分類として実施されてよい。

【００９７】

コンピュータデバイス５０２はまた、携帯電話機、携帯型音楽プレーヤ、携帯型ゲーム機、タブレットコンピュータ、マルチスクリーンコンピュータ、等のようなモバイル機器を含むデバイスのモバイル５１６分類として実施されてよい。コンピュータデバイス５０２はまた、平常の視聴環境において概してより大きいスクリーンを有するか又はそのようなスクリーンへ接続されるデバイスを含むデバイスのテレビジョン５１８分類として実施されてよい。かかるデバイスは、テレビ受像機、セットトップボックス、ゲーム機、等を含む。

【００９８】

ここで記載される技術は、コンピュータデバイス５０２のそれらの様々な構成によってサポートされてよく、ここで記載される技術の具体例に制限されない。例えば、クライアントデバイス１０２及び／又はセキュリティサービス１２０を参照して論じられた機能性は、以下で記載されるように、例えば、プラットフォーム５２２を介して“クラウド”５２０上で、全て又は部分的に分散型システムの使用を通じて実施されてよい。

【００９９】

クラウド５２０は、リソース５２４のためのプラットフォーム５２２を含み且つ／あるいは表す。プラットフォーム５２２は、クラウド５２０のハードウェア（例えば、サーバ）及びソフトウェアの潜在的な機能性を抽象する。リソース５２４は、コンピュータプロセッシングがコンピュータデバイス５０２から遠く離れたサーバで実行されている間に利用されるアプリケーション及び／又はデータを含んでよい。リソース５２４はまた、セルラー又はＷｉ－Ｆｉネットワークのようなサブスクライバネットワークを通じて及び／又はインターネット上で提供されるサービスを含むことができる。

【０１００】

プラットフォーム５２２は、コンピュータデバイス５０２を他のコンピュータデバイス

と接続するリソース及び機能を抽象してよい。プラットフォーム５２２はまた、プラットフォーム５２２を介して実施されるリソース５２４に対する直面されている需要に対する対応するレベルのスケールを提供するためのリソースのスケーリングを抽象する働きをしてよい。然るに、相互接続されるデバイスの実施形態において、ここで記載される機能性の実施は、システム５００の全体にわたって分散されてよい。例えば、機能性は、クラウド５２０の機能性を抽象するプラットフォーム５２２を介して且つコンピュータデバイス５０２において部分的に実施されてよい。

【０１０１】

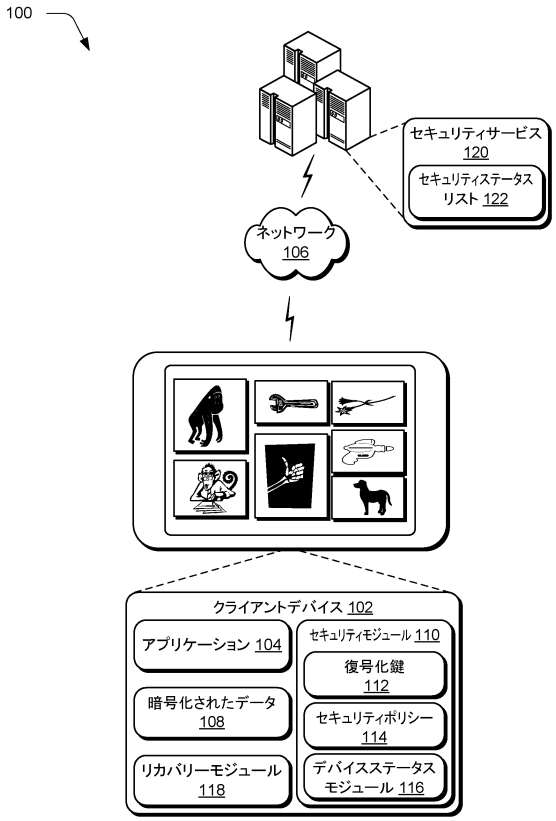
ここで論じられる技術を実行するよう実施され得る多数の方法がここで論じられる。方法の態様は、ハードウェア、ファームウェア、若しくはソフトウェア、又はそれらの組み合わせにおいて実施されてよい。方法は、１以上のデバイスによって実行される動作を特定するブロックの組として示されるが、必ずしも夫々のブロックによって動作を実行するために示された順序に制限されない。更に、特定の方法に関して示されている動作は、１以上の実施に従う異なる方法の動作と組み合わされ及び／又は交換されてよい。方法の態様は、環境１００を参照して上述された様々なエンティティの間のインタラクションを介して実施され得る。

【０１０２】

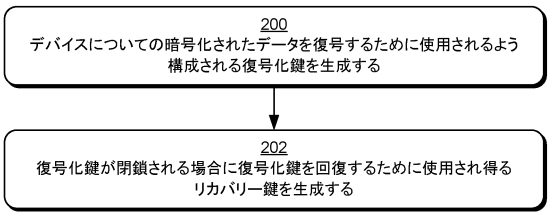
結論

デバイスデータのためのセキュリティポリシーを提供する技術が記載された。たとえ実施形態が構造的特徴及び／又は方法論的動作に特有の言語において記載されるとしても、添付の特許請求の範囲で定義される実施形態は必ずしも、記載されている具体的な特徴又は動作に制限されない点が理解されるべきである。むしろ、具体的な特徴及び動作は、請求される実施形態を実施する例となる形態として開示される。

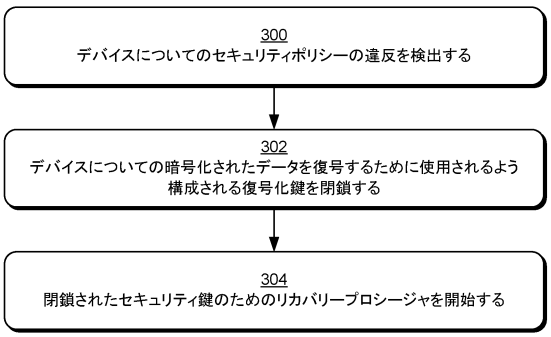
【図１】



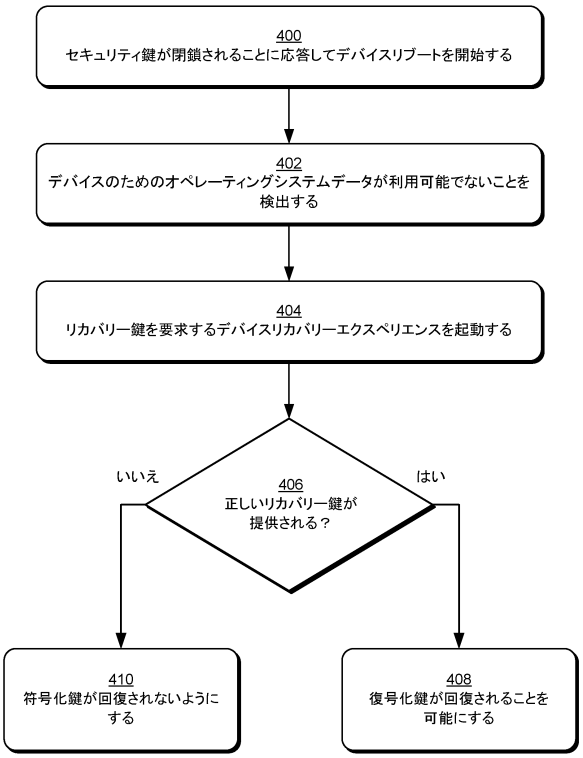
【図２】



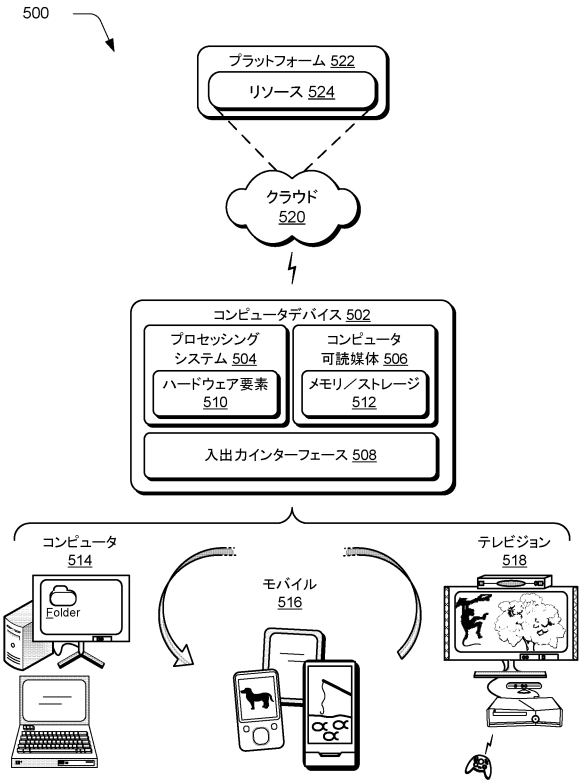
【図３】



【図４】


400
セキュリティ鍵が閉鎖されることに応答してデバイスリブートを開始する
402
デバイスのためのオペレーティングシステムデータが利用可能でないことを検出する
404
リカバリー鍵を要求するデバイスリカバリーエクスペリエンスを起動する
406
正しいリカバリー鍵が提供される？
いいえ
はい
410
符号化鍵が回復されないようにする
408
復号化鍵が回復されることを可能にする

【図５】


500
プラットフォーム 522
リソース 524
クラウド 520
コンピュータデバイス 502
プロセッシングシステム 504
ハードウェア要素 510
コンピュータ可読媒体 506
メモリ／ストレージ 512
入出力インターフェース 508
コンピュータ 514
Folder
モバイル 516
テレビジョン 518

フロントページの続き

(72)発明者 インガルズ, ダスティン, マイケル
アメリカ合衆国 ９８０５２－６３９９ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ 内
(72)発明者 アイド, ネイサン, ジェイ.
アメリカ合衆国 ９８０５２－６３９９ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ 内
(72)発明者 マコーレイ, クリストファー, アール.
アメリカ合衆国 ９８０５２－６３９９ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ 内
(72)発明者 ウレケ, オクタヴィアン, ティー.
アメリカ合衆国 ９８０５２－６３９９ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ 内
(72)発明者 グラス, マイケル ジェイ.
アメリカ合衆国 ９８０５２－６３９９ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ 内
(72)発明者 ヴィナヤク, サイ
アメリカ合衆国 ９８０５２－６３９９ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ 内
(72)発明者 アダム, プレストン, デレク
アメリカ合衆国 ９８０５２－６３９９ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ 内

審査官 金沢 史明

(56)参考文献 特開２０１０－１９１９４６（ＪＰ，Ａ）
特開２００２－０６３１４０（ＪＰ，Ａ）
米国特許出願公開第２００９／０１５０９７０（ＵＳ，Ａ１）
米国特許出願公開第２００９／０００６８６７（ＵＳ，Ａ１）
米国特許出願公開第２００９／０３２８２３８（ＵＳ，Ａ１）
Charlie Russel, Sharon Crawford, Windows Server 2008 オフィシャルマニュアル 下, 日本, 日経ＢＰソフトプレス, ２００９年 3月 2日, 初版, pp. 395-403

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／００－ ９／３８
Ｇ０６Ｆ ２１／００－２１／８８